IPv6 SECURITY

This one-day course provides an overview of the most relevant IPv6 security topics. The participant will gain insight into industry best practice and gain a high-level understanding of the most pressing IPv6 security concerns today. The course includes theory and hands-on exercises.

**Goals**

- Identify what is IPv6 Security and what it isn't
- Identify and protect your network from IPv6-related threats
- Understand how the IPv6-associated protocols work, how to identify them and protect your network from related threats
- Recognise the existing security solutions to protect your IPv6 network
- Understand how to apply packet filtering in IPv6
- Understand how Internet-wide IPv6 threats could happen, such as DDoS or via transition mechanisms
- Understand the many complexities of IPv6 that must be taken into account from a security point-of-view

**Pre-Requisites**

- Laptop with a browser for labs
- For this course you should know about:
  - IPv4 and IPv6 (i.e. RIPE NCC Basic IPv6 Course) networking
  - Basic security concepts
  - For the labs: Linux, CLI and command tools

**Course Content**

- Introduction
- Introduction to IPv6 Security
- Basic IPv6 Protocol Security
  - IPv6 Basic header and EHs
  - Exercise: IPv6 Packet Generation
  - IPv6 Addressing Architecture
  - Exercise: IPv6 Network Scanning
- IPv6 associated protocols security
  - ICMPv6
  - NDP
  - Exercise: NDP Threats
  - MLD
  - DNS
  - DHCPv6
  - IPv6 Routing Protocols
- IPv6 Filtering
  - Filtering IPv6 Traffic
  - Exercise: Filtering IPv6 Traffic
- Internet wide IPv6 threats
  - DDoS
- Transition Mechanisms
- IPv6 Security Tools and Tips

**Online courses:** academy.ripe.net

**Training Services:** www.ripe.net/support/training

**Contact us:** training@ripe.net

**Course Feedback:** www.ripe.net/training/ipv6security/survey

Version: 20190218